

REMARKS

Examiner required updates to the prior art patent applications that are now patents.

Applicants hereby amend the specification to update those patent applications to indicate their patent numbers.

Examiner rejected claims 1-4 under 35 U.S.C. §101 as being directed to non-statutory subject matter. Examiner said that the claims preempt every substantial practical application of the idea that is embodied by the claims. Applicants do no such thing because ideas are not patentable, only devices, methods, compositions of matters, and improvements thereto.

Applicants submit that claims 1-2 concern devices, which are patentable subject matter, and that the components of said devices are described with particularity. Applicants submit that claims 3-4 concern methods, which are patentable subject matter, and that the steps of said methods are described with particularity. Examiner also said that Applicants' device and method are so broad and sweeping as to cover both known and unknown uses of a pseudo-random bit sequence.

Applicants do no such thing. Applicants submit that claims 1-4 only cover the particular devices and methods described in claims 1-4 and nothing else, that any use of a particular pseudo-random bit sequence is not covered by claims 1-4, and that only the particular devices and methods described in claims 1-4 are covered. Examiner suggested amending the claims to include specific implementation of which the claimed invention may be used. Applicants submit that the claims are already specific as to what components make up the devices, what steps make up the methods, and what the devices and methods are used for (i.e., generating an uncorrelated pseudo-random bit sequence uniformly distributed over a user-definable value K , where $K+1$ has m prime factors).

Examiner rejected claims 3-4 under 35 U.S.C. §102 as being anticipated by U.S. Pat. No. 4,780,840 (Van Den Ende).

With regard to claim 3, Examiner said that Van Den Ende discloses Applicants' step of selecting a user-definable value K (Van Den Ende, column 2, lines 53-59). At Examiner's cite, Van Den Ende selects a value 255 (or 2^M in Van Den Erbe, column 4, line 18-29), where the value selected is related to the bit width of the storage locations for the pseudo-random numbers and prime numbers used by Van Den Ende (Van Den Ende, column 2, lines 23-31). Van Den Ende then compares this number to the result of a calculation (Van Den Ende, column 4, lines 17-29, Figure 1, and Figure 2). The number selected by Van Den Ende does not serve the same purpose as the number K selected by Applicants. Applicants select a number that has no relationship to a memory width at which a pseudo-random number or prime number is stored. Applicants do not compare a result of a calculation to K. Instead, Applicants derive prime factors from K+1 (Applicants, page 11, line 9).

Examiner said that Van Den Ende discloses Applicants' step of factoring K+1 into m prime factors (Van Den Ende, column 2, lines 43-59). At Examiner's cite, no factoring of a number occurs. As evidenced by the attached definition from thefreedictionary.com, the word "factor" has multiple definitions. The two relevant definitions are the third and fourth definitions as follows:

One of two or more quantities that divides a given quantity without a remainder. For example, 2 and 3 are factors of 6; and

A quantity by which a stated quantity is multiplied or divided, so as to indicate an increase or decrease in a measurement: The rate increased by a factor of ten.

The first definition of "factor" above concerns a single number that is divided into a series of numbers that if multiplied together would result in the original number. If each number in the series is a prime number then they are prime factors. In the example provided in the first definition above, 2 and 3 are factors of 6. Since 2 and 3 are prime numbers, as evidenced by the

attached definition of prime numbers from odin.mdacc.tmc.edu, they are prime factors. The attachment from home.avvanta.com indicates that this is referred to as “prime factorization.” This is the definition of “factor” used by Applicants.

The second definition of “factor” above concerns a first number that multiplies or divides a second number to change the value of the second number. In the example provided in the second definition above, 10 multiplies a second number to increase the value of the second number by a multiple of 10. This is the definition of “factor” used by Van Den Ende. Van Den Ende expressly calls his “factor” a “multiplication factor” (Van Den Ende, column 3, line 69-column 4 line 1). It is also evident from Figure 2 in Van Den Ende that Van Den Ende is using the second definition above for “factor” and not the first definition as do Applicants. In Examiner’s cite, Van Den Ende mentions prime numbers, but these numbers are not derived from the number selected by Van Den Ende but are read from a memory (Van Den Ende, column 3, line 67). Therefore, Examiner is incorrect that Van Den Ende discloses Applicants’ step of factoring $K+1$ into prime factors.

Examiner said that Van Den Ende discloses Applicants’ step of generating m pseudo-random sequences (Van Den Ende, column 1, lines 38-60). At Examiner’s cite, Van Den Ende generates a (i.e., one) pseudo-random sequence made up of N sub-sequences, where N is user-selected (Van Den Ende, column 3, lines 64-68, Figure 2, column 3, lines 10-16, Figure 1), and not m pseudo-random sequences, where m is the number of prime factors of $K+1$ as do Applicants (Applicants, page 11, lines 7-13).

Examiner said that Van Den Ende generates a pseudo-random sequence $R=r_1+q_1r_2+q_1q_2r_3+\dots+q_1q_2\dots q_{m-1}r_m$ (Van Den Ende, column 3, lines 17-48). Examiner’s cite discloses no such step. Van Den Ende discloses a method of generating a pseudo-random sequence by generating a series of sub-sequences and concatenating them, where each sub-sequence is the sum of a pseudo-random character and a product of a multiplicative factor and a prime number (Van Den Ende, column 3, line 60- column 4, line 56). Applicants do not require the use of a prime number as does Van Den Ende. Applicants determine prime factors from $K+1$,

which is nor required to be a prime number. Van Den Ende's multiplicative factors are not prime factors of $K+1$, and are not even required to be prime numbers (Van Den Ende, column 2, lines 58-59, column 4, lines 29-37, Figure 2). That is, the example in Van Den Ende multiplicative factors are 1 and 2, where 1 is not a prime number (see attachment concerning the definition of a prime number).

In addition, Applicants generate their pseudo-random number by multiplying a series of pseudo-random numbers by a changing group of prime factors (i.e., $q_1, q_1q_2, q_1q_2q_3$, etc.) and then adding the results (Applicants, page 11, lines 14-19), whereas Van Den Ende generates a pseudo-random sequence by generating a series of sub-sequences and concatenating them, where each subsequence is the sum of a pseudo-random character and a product of a multiplicative factor selected from the group of two factors and a prime number (Van Den Ende, column 3, line 60- column 4, line 56).

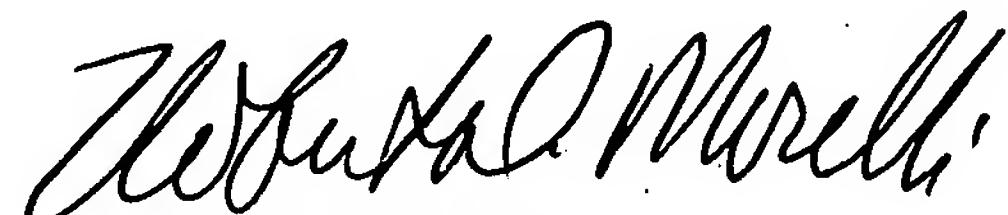
With regard to claim 4, Examiner said that Van Den Ende discloses Applicants' step of factoring $K+1$ into m prime factors q_1, q_2, \dots, q_m , where q_1, q_2, \dots, q_m are ordered from smallest values to largest value (Van Den Ende, column 2, line 60-column 3, line 16). At Examiner's cite, Van Den Ende stores sub-sequences in a memory in the order in which they were generated, not by their value. In addition, the sub-sequences generated by Van Den Ende are not prime factors of $K+1$. Van Den Ende does not factor $K+1$ into prime factors. Van Den Ende cannot order by value that which he does not generate in the first place. Therefore, Examiner is incorrect that Van Den Ende discloses this step.

Applicants hereby amend their application in light of Examiner's rejections.

Reconsideration of the application in light of the amendment and the remarks is requested.

Applicants request Examiner withdraw his rejections and allow claims 1-4.

Respectfully submitted,


Robert D. Morelli
Registration No. 37,398
(301) 688-0287

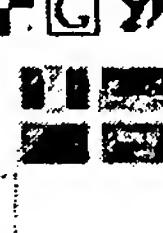


592,342,668 people served.

[TheFreeDictionary](#) [Google](#)

factor

Search

[Word / Article](#) [Starts with](#) [Ends with](#) [Text](#)


• Dictionary thesaurus	• Computing dictionary	Medical dictionary	• Legal dictionary	• Financial dictionary	• Acronyms	• Idiom	Columbia encyclopedia	■ Wikipedia encyclopedia
--	--	------------------------------------	------------------------------------	--	----------------------------	-------------------------	---------------------------------------	--

factor Also found in: Computing, Medical, Legal, Financial, Acronyms, Columbia, Wikipedia, Hutchinson 0.0

Factor Business Receivables

Sponsored links

No Obligation. Free Consultation. 25 Years Experience. Discounts as Low as 1.5%.

www.factor4cash.net

Factor-30 Day Free Trial

New Century Financial provides customized cash flow solutions nationwide through its Just In Time Cash service. Get 24 hour convenient online factoring proposal from the No Fees Guys.

www.new-century-financial.com

Get the Cash You Need Today

Factoring. Use your customers credit to get cash. **Factor** your invoices. Fast and easy, no upfront fees, startups/past credit problems OK. Call CapitalPlus today.

www.capitalplus.com

Page tools



[Printer friendly](#)

[Cite./ link](#)

[Email](#)

[Feedback](#)

Introducing



Time saving
tools help
you get
better
information
faster.

Try it now

factor

n.

1. One that actively contributes to an accomplishment, result, or process: "Surprise is the greatest factor in war" Tom Clancy. See Synonyms at element.
2.
 - a. One who acts for someone else; an agent.
 - b. A person or firm that accepts accounts receivable as security for short-term loans.
3. *Mathematics* One of two or more quantities that divides a given quantity without a remainder. For example, 2 and 3 are factors of 6; a and b are factors of ab.
4. A quantity by which a stated quantity is multiplied or divided, so as to indicate an increase or decrease in a measurement: *The rate increased by a factor of ten.*
5. A gene. No longer in technical usage.
6. *Physiology* A substance that functions in a specific biochemical reaction or bodily process, such as blood coagulation.

tr.v. factored, factoring, factors

To determine or indicate explicitly the factors of.

Phrasal Verb:

factor in

To figure in: *We factored sick days and vacations in when we prepared the work schedule.*

[Middle English factour, *perpetrator, agent*, from Old French facteur, from Latin factor, *maker*, from facere, *to make*; see dhé- in Indo-European roots.]

Prime Numbers

Mathematicians have a special fondness for definitions. The objects they study often have no physical presence: you can't touch them, weigh them, or smell them. So, precise definitions are used to provide a solid underpinning to their subject. Definitions are made for two reasons. Sometimes a mathematician makes a definition in order to have a simple shorthand term for a more complicated object that was needed to make sense of a proof. In other cases, a definition is a kind of generalization, made to unite lots of examples and special cases into a single kind of thing deserving further study. In the present document, we want to investigate some of the consequences of a single, simple definition of the latter kind.

Definition: An integer p is called a *prime* number if the only positive integers that divide p are 1 and p itself. Integers that are not prime are called *composite*.

Here are the first few prime numbers:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

Prime numbers are special because they are the elementary building blocks of the multiplicative structure on the integers; every integer can be written in only one way as a product of its prime factors. The mathematically precise version of this assertion is known as the The Fundamental Theorem of Arithmetic.

There are a number of interesting questions you can ask about prime numbers and factorizations.

- Given any integer n , how do you find its prime factorization?
- Given any integer n , how do you decide if it is a prime number?
- How many prime numbers are there?
- Can you list all the prime numbers less than a given bound?

[\[Home Page\]](#) [\[Bioinformatics\]](#) [\[Mathematics\]](#) [\[Creative Efforts\]](#)

[\[HOME\]](#) [\[PREVIOUS\]](#) [\[NEXT\]](#) [\[UP\]](#) [\[DOWN\]](#)

Disclaimer: This page was last updated on 12 October 2002. It is entirely possible that the information contained herein no longer has any connection with reality (assuming it ever did). Feel free to send



- **Prime factorization**

Prime factorization is finding the factors of a number that are all prime. Here's how you do it: Find 2 factors of your number. Then look at your 2 factors and determine if one or both of them is not prime. If it is not a prime factor it. Repeat this process until all your factors are prime. Here's an example:

Find the prime factors of the number 84:

```
84
  / \
42 x 2  (84 is 42 times 2)
  / \
21 x 2  (42 is 21 times 2)
  / \
7 x 3   (21 is 7 times 3)

(7 and 3 are both prime, so we stop!)
```

So the prime factors of 84 are $7 \times 3 \times 2 \times 2$.

Now, here's a problem for you: Find the prime factors of 60.

Use your browser's **BACK** button to go back
...or go to the index of definitions
...or go back to the home page